National Aeronautics and
Space Administration

Office of the Administrator
Washington, DC 20546-0001

July 26, 2006

TO: Officials-in-Charge of Headquarters Offices
Directors, NASA Centers

FROM: Deputy Administrator

SUBJECT: Meeting NASA Information Technology Security Requirements

Due to an increasing number of information technology (IT) security and privacy information-related incidents reported across the Government, I am hereby directing a comprehensive IT security review be conducted within NASA to assess and ensure the level of integrity of NASA IT systems. The review will:

- Assess the level to which NASA Headquarters and each NASA Center is meeting existing requirements as stipulated in NASA Procedural Requirements (NPR) 2810.1A, "Security of Information Technology," and NPR 1600.1, "NASA Security Program Procedural Requirements."

- Evaluate the effectiveness of NASA Headquarters and each Center's IT security organizational structure.

- Verify the accuracy of NASA Headquarters and each Center's IT security incident and status reports.

- Evaluate the effectiveness of NASA Headquarters and each Center's policy enforcement efforts.

A review team will be assembled from experts across the appropriate organizations within NASA and will begin its review within two weeks from the issuance of this memorandum. Your cooperation is appreciated.

Additionally, to ensure that all NASA information and IT resources are meeting Federal IT security requirements and best practices, I am directing the actions listed below be given your full support. The list is separated into actions tied to existing requirements, and actions tied to new requirements established immediately by virtue of this memorandum.

Existing Requirements:

1. Ensure all NASA IT systems comply with NPR 2810.1A by March 2007. Required actions include:

    a. Developing and maintaining accurate information on all NASA systems and documenting this information in approved IT System Security Plans.

    b. Managing risks at the appropriate level of detail and acceptance of residual risk by management at the appropriate level of seniority.

    c. Addressing IT security concerns in all phases of the system development life cycle.

    d. Implementing and verifying security controls through the established NASA certification and accreditation process and through annual IT security assessments of all systems containing NASA information and data.

2. Ensure routine vulnerability scans of all NASA IT system components and devices using the NASA standard vulnerability scanning solution(s) are conducted.

3. Ensure the operating systems and applications of all NASA IT system components and devices comply with NASA's established operating system, application standards, and configuration guidelines; maintain all operating systems and application software, at the current patch level, verified using the NASA patch management solution.

4. Ensure Incident Handling and Reporting is conducted according to NPR 2810.1A. Each Center Director will ensure all IT security incidents are accurately reported to the Center IT Security Manager, who will then report all available information, at the device level, to the NASA Security Incident Reporting Center.

5. Ensure Agency intrusion detection systems and network monitoring solutions at all system and network interconnections are properly supported.

6. Ensure approved NASA remote access methodologies are followed. The current requirements have been established by each NASA Center.

Each NASA Center is currently required to submit a Federal Information Security Management Act (FISMA) Quarterly Status Report to the Office of the CIO. This report, in part, indicates the Center's status in meeting the above requirements. Center Directors are to ensure the accuracy of the Center's FISMA Quarterly Status Report submissions. The next report is due on September 1, 2006. This report serves as an opportunity for Centers to identify any challenges in meeting the existing requirements.

New Requirements:

For each of the new requirements listed below, the Office of the CIO will work with your Center CIO to establish an implementation plan and the appropriate mechanisms to track your Center's or Program's performance against the plan.

1. In addition to the existing Incident Handling and Reporting requirements in NPR 2810.1A, all incidents involving personally identifiable information shall be reported within one hour of detection.

2. Following the approval of each Center's Migration Plan by the NASA CIO, implement Active Directory trusts and network interconnections based on the approved NASA Architecture Design. All new implementations shall meet the approved NASA Architecture Design for Active Directory.

3. All systems and applications classified according to Federal Information Processing Standards 199 and National Institutes of Standards and Technology Special Publication 800-60 as being Moderate or High are required to utilize two-factor authentication. All NASA systems and applications are required to only allow two-factor authentication used in conjunction with the Internet Protocol Security to administer servers and network devices. This is the standard access control process to be followed for remote administration of NASA IT systems, including the prohibition of "server hopping" to administer servers. (Note: Historically, NASA has used "SecurID" tokens for two-factor authentication. As the Agency implements Homeland Security Presidential Directive [HSPD]-12, two-factor authentication based on Public Key Infrastructure [PKI] and Smartcards will become the standard. Therefore, any system or application rated High or Moderate that is not currently protected by two-factor authentication should be placed on the priority list for HSPD-12, PKI, and Smartcard implementation.)

4. Ensure all contracts include NASA's strengthened IT Security Clause. The new clause is currently undergoing approval through the Federal rule-making process. Until approved, new contracts shall contain the language of the clause within the contract requirements. After the clause is approved, existing contracts should be modified to include the strengthened IT Security Clause, unless expressly waived in writing by the NASA Assistant Administrator for Procurement in coordination with the NASA CIO.

5. In order to achieve consistency in how NASA is meeting IT security requirements as defined in NPR 2810.1A, all Center Directors are to designate a representative to participate in the formulation and review of IT Security Standard Operating Processes (ITS-SOPs) and then ensure approved ITS-SOPs are followed.

6. Ensure frequent review of operating system and application logs to identify unauthorized and anomalous activity. Where appropriate, use a centralized logging

capability to maintain the integrity of the logs. Logs should be kept for a minimum of one year.

7. Limit administrative rights and privileged accounts to only those employees requiring them, and periodically review those with administrative privileges to ensure that administrative rights are still required.

Due to the seriousness of this matter, the NASA CIO has the responsibility and the authority to disconnect any NASA systems (and/or non-NASA IT systems connected to NASA networks), both institutional and programmatic, not meeting all requirements within an appropriate timeframe, as determined by the NASA CIO in consultation with the system owner. Non-compliant systems will remain disconnected until they are brought into compliance.

Please address questions to Scott Santiago, Deputy Chief Information Officer for Information Security Technology, at scott.santiago@nasa.gov or (202) 358-1377. Center-specific or technical questions may also be directed to the Center CIOs or Center IT Security Managers.

Shana Dale